



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/902,520	07/10/2001	Jose' C. Brustoloni		7438

7590

11/26/2004

Docket Administrator
Lucent Technologies Inc.
Room 3J-219
101 Crawfords Corner Rd.
Holmdel, NJ 07733-3030

EXAMINER

ANANTHANARAYANAN, RAMYA

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 11/26/2004

6

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/902,520

Applicant(s)

BRUSTOLONI, JOSE' C.

Examiner

Ramya Ananthanarayanan

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03 July 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-34 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-34 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 11 July 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Art Unit: 2131

1. Claims 1-34 have been examined.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on July 13, 2001 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

3. The abstract of the disclosure is objected to because it is longer than the specified 150 words in length. Correction is required. See MPEP § 608.01(b).
4. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01. The hyperlink is located on page 6, line 9 of the specification.
5. The disclosure is objected to because of the following informalities: On page 20, line 8 of the specification, a typographical error was found. The client software mentioned in the specification is depicted in item 320, not in item 325 as stated. On page 25, line 18, the word "note" should be "noted" in the phrase "the same value as PINGTRIES note above."
6. Appropriate correction is required.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1, 2, 6, 18, 19, and 23 are rejected under 35 U.S.C. 102(b) as being anticipated by Birrell et al. (U. S. Patent 5,805,803).

9. With respect to claims 1 and 18, Birrell et al. disclose a method in program code used with a computer readable media (column 2, lines 21-22) comprising:

Sending a control packet from a first endpoint of a tunnel through the tunnel to a second endpoint of the tunnel; and

Waiting at the first endpoint for a responsive control packet through the tunnel from the second endpoint before sending packets other than a control packet through the tunnel. (Figure 2, column 4, paragraphs 1-9).

10. With respect to claims 2 and 19, Birrell et al. disclose further the method in program code used with a computer readable media (column 2, lines 21-22) wherein the tunnel is a secure tunnel (column 4, line 67 to column 5, line 1).

11. With respect to claims 6 and 23, Birrell et al. further disclose the method in program code used with a computer readable media (column 2, lines 21-22)

Art Unit: 2131

wherein the first endpoint is a client and the second endpoint is a server (column 3, lines 61-64).

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102

that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

13. Claims 1-5, 7-10, 18-22, and 24-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Bendinelli et al. (U. S. Publication 2002/0029276).

14. With respect to claims 1 and 18, Bendinelli et al. disclose a method in program code used with a computer readable media (paragraphs 0019 and 0020) comprising:

Sending a control packet from a first endpoint of a tunnel through the tunnel to a second endpoint of the tunnel; and

Waiting at the first endpoint for a responsive control packet through the tunnel from the second endpoint before sending packets other than a control packet through the tunnel.

(Bendinelli discloses that his method utilizes the SSL (Secure Sockets Layer) protocol handshake [Paragraph 0157 lines 6-7] in which the client sends a

Art Unit: 2131

control message to the server and after receiving the message the server responds. This send and response of control packets continue in a specific manner as detailed in the SSL Version 3 specification and then the client and server have completed the handshake and may send data packets. An overview of the handshake protocol can be found in Section 5.5.)

15. With respect to claims 2, 3, 19 and 20, Bendinelli et al. disclose further the method in program code used with a computer readable media (paragraphs 0019 and 0020) wherein the tunnel is a secure tunnel and uses the IPSec security protocol suite. (In paragraph 0180 line 12, Bendinelli discloses that the tunnel uses the IPSEC security protocol, meaning that the tunnel is secure.)

16. With respect to claims 4 and 21, Bendinelli et al. disclose further the method in program code used with a computer readable media (paragraphs 0019 and 0020) wherein the tunnel uses ESP in tunnel mode (In paragraph 0349, Bendinelli discloses the format of the IPSec packet and header. The description given matches with the ESP tunnel mode implementation of the IPSec security protocol suite as disclosed in Section 3.1 of RFC 2406 of the IETF, in which when ESP is employed, protection is offered only to the inner header, not to the IP packet's outer header and other layers as in AH.).

17. With respect to claims 5 and 22, Bendinelli et al. further disclose the method in program code used with a computer readable media (paragraphs 0019 and

Art Unit: 2131

0020) wherein the tunnel traverses at least one network address translator (paragraph 0141, lines 5-13).

18. With respect to claims 7 and 24, Bendinelli et al. further disclose the method in program code used with a computer readable media (paragraphs 0019 and 0020) wherein the NAT implements VPN Masquerade (In the third paragraph of the Linux VPN Masquerade website admitted as prior art by applicant, it states that VPN Masquerade is a part of IP Masquerade which enables to use IPSec-based VPN clients. In paragraph 0141, lines 14-17, Bendinelli discloses that IP Masquerade will be facilitated for use with NAT, after disclosing an environment using VPN and IPSec.).

19. With respect to claims 8 and 25, Bendinelli et al. disclose a method in program code used with a computer readable media (paragraphs 0019 and 0020) comprising: sending a control packet from a first endpoint of a tunnel through the tunnel to a second endpoint of the tunnel (paragraph 0389, lines 7-9) and waiting at the first endpoint for a responsive control packet through the tunnel from the second endpoint (paragraph 0389, lines 9-10) before sending packets other than a control packet through the tunnel (paragraph 0389, lines 18-20). Bendinelli further discloses that the control packets being sent through the tunnel are ICMP packets (paragraph 0389, lines 7-9).

Art Unit: 2131

20. With respect to claims 9, 10, 26 and 27, Bendinelli et al. further disclose the method in program code used with a computer readable media (paragraphs 0019 and 0020) wherein the tunnel is defined by an epoch, the epoch comprising one security association (SA) in each direction, each SA having a negotiated limited lifetime, wherein before the end of the tunnel's lifetime the endpoints establish a new tunnel between them, and defining the use of the ESP protocol in tunnel mode with negotiated authentication and/or encryption keys and with a security parameters index (SPI) chosen by the SA's destination.

(It is inherent in the usage of IPSEC and ESP in tunnel-mode in claims 3 and 4 that security associations must also be used (RFC 2401 from the IETF, Section 4). By using the tunnel to communicate from and to the gateway, it is inherent that security associations were established in both directions (RFC 2401 from the IETF, Section 4.1, lines 6-8). It is also inherent in a security association to have negotiated authentication and/or encryption keys (RFC 2401 from the IETF, page 21, bullet 5) with a security parameters index SPI (RFC 2401 from the IETF, Section 5.2, paragraph 2, lines 1-2) chosen by the destination (RFC 2401 from the IETF, Section 4.7, lines 1-3). Additionally, it is inherent in a security association utilizing ESP to have a negotiated limited lifetime wherein before the end of the tunnel's lifetime, the security association is rekeyed with a new SPI and the endpoints have in essence established a new tunnel (RFC 2401 from the IETF, page 21, bullet 7, explanation of lifetimes)).

Art Unit: 2131

21. Claims 1-6, 9-10, 18-23, and 26-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Brustoloni et al. (Publication no. 2001/0034831).

22. The applied reference has a common inventor with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not the invention "by another," or by an appropriate showing under 37 CFR 1.131.

23. With respect to claims 1 and 18, Brustoloni et al. disclose a method in program code used with a computer readable media (paragraphs 0023 and 0024) comprising:

Sending a control packet from a first endpoint of a tunnel through the tunnel to a second endpoint of the tunnel; and

Waiting at the first endpoint for a responsive control packet through the tunnel from the second endpoint before sending packets other than a control packet through the tunnel.

(Brustoloni discloses that his method utilizes the SSL (Secure Sockets Layer) protocol handshake [Paragraph 0085 lines 7-8] in which the client sends a control message to the server and after receiving the message the server responds. This send and response of control packets continue in a specific

Art Unit: 2131

manner as detailed in the SSL Version 3 specification and then the client and server have completed the handshake and may send data packets. An overview of the handshake protocol can be found in Section 5.5.)

24. With respect to claims 2, 3, 19 and 20, Brustoloni et al. disclose further the method in program code used with a computer readable media (paragraphs 0023 and 0024) wherein the tunnel is a secure tunnel and uses the IPsec security protocol suite. (In paragraph 0084, line 2 and paragraph 0066, lines 4-5, Bendinelli discloses that the tunnel is a secure tunnel that uses the IPSEC security protocol.)

25. With respect to claims 4 and 21, Brustoloni et al. disclose further the method in program code used with a computer readable media (paragraphs 0023 and 0024) wherein the tunnel uses ESP in tunnel mode (paragraph 0083, lines 4-8).

26. With respect to claims 5 and 22, Brustoloni et al. further disclose the method in program code used with a computer readable media (paragraphs 0023 and 0024) wherein the tunnel traverses at least one network address translator (NAT) (paragraph 0061, line 5).

27. With respect to claims 6 and 23, Brustoloni et al. further disclose the method in program code used with a computer readable media (paragraphs 0023 and

Art Unit: 2131

0024) wherein the first endpoint is a client and the second endpoint is a server (paragraph 0047, lines 8-15).

28. With respect to claims 9, 10, 26, and 27, Brustoloni et al. further disclose the method in program code used with a computer readable media (paragraphs 0023 and 0024) wherein the tunnel is defined by an epoch, the epoch comprising one security association (SA) in each direction, each SA having a negotiated limited lifetime (wherein before the end of the tunnel's lifetime the endpoints establish a new tunnel between them) and defining the use of the ESP protocol in tunnel mode with negotiated authentication and/or encryption keys and with a security parameters index (SPI) chosen by the SA's destination.

(It is inherent in a security association to have a negotiated limited lifetime wherein before the end of the tunnel's lifetime, the security association is rekeyed with a new SPI and the endpoints have in essence established a new tunnel (RFC 2401 from the IETF, page 21, bullet 7 explanation of lifetimes)).

Claim Rejections - 35 USC § 103

29. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2131

30. Claims 11-12, 14, 15, 28-29, 31 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bendinelli et al. (U. S. Publication 2002/0029276) as applied to claims 1-4 and 18-21 above, and further in view of Rabenko et al (U.S. Patent 6,765,913).

31. Bendinelli et al. disclose the limitations set forth in claims 1-4 and 18-21, upon which claims 11-12, 14-15, 28-29, 31, and 32 are dependent. However, Bendinelli et al. do not disclose the limitations set forth in claims 11-12 (or the corresponding claims 26-29). Bendinelli et al. further do not disclose the limitations set forth in claims 14 and 15 (or corresponding claims 31 and 32). Rabenko et al. disclose the limitations set forth in claims 11-12, 14-15, 28-29, 31, and 32.

32. Both Bendinelli et al. and Rabenko et al. are analogous art because both are in the field of secure data communications networks.

33. With respect to claim 11 and 28, Rabenko et al. further disclose the method in a computer readable medium (column 9, line 6-8) wherein a designated endpoint has responsibility for establishing the new tunnel and ignores requests initiated by the other endpoint to establish the tunnel (column 19, lines 37-41, 44-48).

Art Unit: 2131

34. With respect to claim 12 and 29, Rabenko et al. further disclose the method in a computer readable medium (column 9, line 6-8) wherein the second endpoint waits for a packet from the first endpoint through the tunnel before using the tunnel to send any packets (column 97, lines 16-19).

35. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine these teachings of Rabenko et al. with the method of Bendinelli et al. in order to reduce the possibility of race conditions, as described in applicant's specification.

36. With respect to claims 14, 15, 31, and 32, Rabenko et al. further disclose the method in a computer readable medium (column 9, line 6-8) wherein the first endpoint sends through the tunnel to the second endpoint a predetermined maximum number of control packets without receiving any packets through the tunnel then the first endpoint establishes a new tunnel to the second endpoint. Rabenko et al. additionally further disclose the method wherein if an endpoint is unable to complete the establishment of a new tunnel before a predetermined time limit then that endpoint abandons establishment of that tunnel and starts establishing a new tunnel (column 97, lines 19-37).

37. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the recovery methods of Rabenko et al. with the system of

Art Unit: 2131

Bendinelli in order to provide automatic recovery from a NAT crash or race conditions, as described in applicant's specification.

38. Claims 13 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Birrell et al. (U. S. Patent 5,805,803) as applied to claims 1 and 18 above, and further in view of Capurka et al. (U. S. Patent 6,678,258).

39. With respect to claims 13 and 30, Capurka et al. further disclose the method in computer readable medium (column 3, lines 48-53) wherein if the first endpoint does not receive any packets through the tunnel for a predetermined time interval then the first endpoint sends through the tunnel a control packet to the second endpoint (column 2, lines 65-67 to column 3, line 1).

40. Birrell et al. and Capurka et al. are analogous art because both deal with the field of packet data communication systems. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the method of Birrell et al. with the method of Capurka et al. in order to provide a recovery method for the system.

41. Claims 16, 17, 33, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bendinelli et al. (U. S. Publication 2001/0034831) and Rabenko et al. (U. S. Patent 6, 765, 931) as applied to claims 1-3, 9-10, 15, 18-

Art Unit: 2131

20, 26, 27, and 32 above, and further in view of Ogier et al. (U. S. Publication 2003/0179742).

42. The combination of Bendinelli et al. and Rabenko et al. disclose the limitations set forth in claims 1-3, 9-10, 15, 18-20, 26, 27, and 32, upon which claims 16, 17, 33, and 34 are dependent. However, the combination of Bendinelli et al. and Rabenko et al. do not disclose the limitations set forth in claims 16-17 (or the corresponding claims 33-34). Ogier et al. disclose the limitations set forth in claims 15-16 and 33-34.

43. With respect to claims 16, 17, 33, and 34, Ogier et al. further disclose the method in a computer readable medium (The method is implemented in the internetworking system which is made up of subnets (paragraph 0053, lines 1-2), which are in turn made up of nodes (paragraph 0055, lines 6-10). Nodes, as disclosed by Ogier et al. in paragraph 0384, are a computer readable medium.) wherein if an endpoint successively fails to establish a new tunnel before a predetermined maximum number of times then that endpoint closes the connection currently being used to establish tunnels with the other endpoint and opens another such connection (paragraph 0361, lines 1-12) wherein the connection is an IKE session (Bendinelli: paragraph 0187, lines 4-6; paragraph 0188, lines 6-9).

Art Unit: 2131

44. Bendinelli et al., Rabenko et al. and Ogier et al. are all analogous art because all deal with the field of secure data communications networks. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the method of Ogier et al. with the combined system of Bendinelli et al. and Rabenko et al. in order to provide fail-over recovery from a crash of the NAT.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ramya Ananthanarayanan whose telephone number is (571) 272-5860. The examiner can normally be reached on Monday through Friday, 8:30-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

RA


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100